PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of LENZARINI

Application No. Examiner:

Filed: Herewith Group Art Unit:

For: METHOD AND SYSTEM FOR SEAMLESS HANDOVER OF MOBILE DEVICES IN HETEROGENEOUS NETWORKS

SUBMISSION OF ANNEXES TO INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY (CHAPTER II)

Commissioner for Patents
P O Box 1450
Alexandria, VA 22213-1450

Sir:

Please find enclosed a copy of the Annexes to the International Preliminary Report on Patentability (Chapter II) including amendments to the specification and claims. Please note that the amendments to the claims presented herein are for informational purposes only, as they are superceded by a Preliminary Amendment filed herewith.

Respectfully submitted,

Dated: 8/10/06

/Sarah E. Smith/
Mark D. Passler
Registration No. 40,764
Sarah E. Smith
Registration No. 50,488
AKERMAN SENTERFITT
Post Office Box 3188
West Palm Beach, FL 33402-3188
Tel: (561) 653-5000

(94) As mentioned, in the prior art we can find the following eight patent applications, which can be regarded as representing the prior art for the issue of avoiding the client application shutdown during the wireless network connection switches. These are WO 02/103978 A2 (Swisscom Mobile AG), EP 1 089 495 A2 (Nortel Networks Limited), EP 0 998 094 A2 (Nokia Mobile Phones LTD), WO 03/065682 A1 and WO 03/065654 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V.), WO 02/43348 A1 (Columbitech AB), EP 1 322 089 A2 (Theodoros Assimakopoulos) and US 2002/0147832 A1 (Saint-Hilaire et al). All these patent applications, except WO 02/43348 A1 and EP 1 322 089 A2, make use of the concept of Mobile IP as described in IP Mobility Support – IETF RFC 2002 (C. Perkins - IBM IP Mobility Support - IETF RFC 2002 - October 1996). Internet makes use of the IP (Internet Protocol) to route data packets (datagrams) from the source to the destination. The source and the destination must have an IP address unique in Internet in order to be reached, something like the telephone number in the telephony world. When the destination address of the data packets is a mobile node this means that a new IP network address must be assigned with each change of network location, which makes transparent mobile accesses impossible. These mobility problems were solved by the Mobile IP standard of the IETF. Mobile IP allows the mobile node to use two IP addresses. One of these addresses is the normal, static IP address (home address), which indicates the location of the home network, whereas the second is a dynamic IP care-of address, which provides information about its current point of attachment to the Internet. The assignment of the two addresses allows the IP data packets to be rerouted to the correct, momentary address of the mobile node. The Mobile IP provides for registering the care-of address with a Home Agent. The Home Agent is normally a fixed network node, which administers the two addresses of the mobile node (home address and care-of address) and reroutes or routes the corresponding data packets: it sends datagrams destined for the mobile node through an IP tunnel to the care-of address. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node.

Unfortunately, the Mobile IP of the IETF does not solve all the mobility problems: if, for instance, a user would like to switch between two different network interfaces while an IP application is running, the IP connection

is interrupted at the moment when he leaves the old network link This connection is interrupted at least until the new location, i.e the new care-of

running the client or the server application and not on different devices This Session Mobility gives the possibility to handle the security at Session Layer, making possible to provide VPN solutions to enforce strong end-to-end security on an application-to-application level but its major drawback is that it lacks in architectural flexibility, requiring the adapted Session Layer to be installed in any devices involved in the communication

The patent application EP 1 322 089 describes an apparatus and a system for dynamically attaching wireless mobile stations to Internet Protocol networks, overcoming various performance problems of the TCP protocol when used on wireless connections through the introduction of a new single protocol relay station called Mobile Access Router Controller (MARC) between the mobile station (MS) and the correspondent host (CH). This relay station contains a so-called *Socklets server* and a *Protocol Relay* module The *Socklets Server* on the MARC corresponds to a so-called *Socklets Client* on the mobile device. The *Socklets Client* replaces the operating system BSD socket API and makes available all methods provided by the original operating system BSD socket API Thus, all applications continue to work without the need for any modification. The *Socklets Client* intercepts all calls from the mobile device applications before their transmission to the network The *Socklets Client* then generates data units called *Socklets-PDU*, encapsulating the original data sent by the applications These *Socklets-PDUs* are sent on the network connection between the *Socklets Client* on the mobile device and the *Socklets Server* on the MARC using optimised custom layer 2, 3 and 4 protocols and not using the traditional TCP/IP or UDP/IP protocol stack. Once on the MARC, the *Protocol Relay* module uses the *Socklets-PDUs* received from the *Socklet's Client* and transformed by the *Socklets Server* to make the traditional TCP(UDP) calls used to establish or destroy sockets with the correspondent host (CH) and to send or receive data to or from it However, the use of proprietary protocols implies that proprietary equipment has to be used, as Internet routers are not able to forward the *Socklet-PDUs* Moreover, a lot of operating system changes make the solution highly platform dependent, while performed OSI layer modification can cause compatibility problems with VPN implementations.

The patent application US 2002/0147832 discloses a method for framing and processing messages in order to achieve, among other things, the data transmission without loss of information when switching from one network connection to another. The objective of the presented solution is an improvement of the Mobile IP (IETF RFC 2002), which allows a mobile agent to be connected to the home network using the same IP home address regardless of its physical location. This objective is achieved mainly through the introduction of a framing and processing unit on both the mobile agent and the home agent side. These units intercept the traffic between the applications running on the mobile agent and the home applications running on the home network, and perform framing and processing of the information in order to provide services such as resistance to a loss of connection, reliable traffic handoff in the case of a connection switch, stream aggregation, compression, security, quality of service and/or roundtrip and bandwidth optimisation. The framing activity uses a particular protocol, and appends a header to each application fragment in order to be used and transferred between the two units. An improvement of the Mobile IP technique is guaranteed through the introduction of a so-called *Mobility Buffer/ACK* unit that provides a reliable transfer of data also in the case of a network connection switch. This *Mobility Buffer/ACK* is used both on the mobile agent and home agent side to store outgoing information until the counterpart acknowledges the successful reception of the information. Finally, a *Firewall Traversal* unit is used on both transmission sides to compress/decompress, encrypt/decrypt and to wrap the information to make it appear as HTTP traffic, so that it can pass through firewalls. The solution according to this US patent application has the same drawbacks as all the solutions based on the Mobile IP concept plus further drawbacks not related to use of Mobile IP, such as a double encapsulation (one due to the Mobile IP and another one due to the framing activity) resulting in an increase of transmission costs due to the additional data to be exchanged and a decrease of the throughput due to the IP fragmentation problems. In addition, the use of the described *Firewall Traversal* unit adds a further encapsulation level needed for wrapping the data in order to make it appear as HTTP traffic. This solution introduces a second level of reliability to the TCP/IP reliability

mechanism, already based on the reception of an acknowledgement by the sender in order to consider the transmission successfully done This second reliability level reduces considerably the throughput of the connection, especially in the case of wireless connections with high latency and thus with high round trip time, as the sender has to wait for both the first (regular TCP) and the second level acknowledgement in order to consider the transmission successfully completed

Finally the mentioned document "Supporting CORBA Applications in a Mobile Environment" MOBICOM '99 by HAAHR M et al. is only one of the numerous solutions providing the seamless handover by offering to the client and server application developers a software framework with a set of API to be used. The major drawback of this kind of solutions is the backward compatibility The seamless handover can be granted only if the client and server applications have been developed using the provided software framework. All the already developed and largely used client and server applications can't enjoy the seamless mobility.

Summary of the Invention

It is an object of this invention to propose a new method and system for seamless handover of mobile devices in heterogeneous networks In particular the switching from one network connection to another should be carried out without interruption of the IP applications and makes possible an uninterrupted continuation of the program course also with real-time applications, if applicable, without being dependent upon specific protocols or network technologies or operating systems. Therefore, it is an object of this invention to provide a method and a system capable of managing, without being dependent upon different protocols or network technologies or operating systems, an automatic/semi-automatic and transparent handover between different network access technologies and/or access providers without interrupting active network applications or sessions.

This object is attained according to the present invention through the elements of the independent claims Further preferred embodiments follow, moreover, from the dependent claims and from the description

IP application (11) and bound to the IP address provided by a first physical interface used to communicate with the Client IP application (11), and a client application emulation interface composed of sockets and server sockets used to exchange data with the server-service module (22) and bound to the IP address provided by a second physical interface currently selected by the client-service module (12).

47. System according to the claim 44 or 46, characterised in that the server-service module (22) comprises at least a server application emulation interface composed of sockets and server sockets used to exchange data with the client-service module (12) and a client application emulation interface composed of sockets and server sockets used to exchange data with the Server IP application (21)

48. System according to the claim 47, characterised in that a plurality of client-service modules (12) of two or more mobile devices, providing client service emulator server sockets on the same ports, is connected to the same server-service module (22) and the client application emulation interface sockets of the server-service module (22) are bound to different Virtual IP addresses created and/or allocated by it

49. System according to any one of the claims 37 to 48, characterised in that the system comprises the server-service module (22) installed on the same device (20) as the Server IP application (21).

50. System according to any one of the claims 37 to 48, characterised in that the system comprises the server-service module (22) installed on a different device of the same network as the device (20) running the Server IP application (21).

51. System according to any one of the claims 37 to 48, characterised in that the system comprises the server-service module (22) installed on any Internet node